					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P05					Názov dokumentu: **Politika riadenia zmien**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1, 5	Rieši opatrenia na zvládanie rizík, riadenie prístupu a riadenie zmien
ISO/IEC 27002:2022	Kontrola 8	Zavádza štruktúrovaný proces riadenia zmien
NIST SP 800-53 Rev.5	CM-2 až CM-14	Kontroly riadenia konfigurácie
Nariadenie EÚ GDPR	Články 32(1)(b–d), 25; odôvodnenie 78	Technické a organizačné opatrenia na bezpečnosť systémov a údajov počas zmien
Smernica EÚ NIS2	Článok 21(2)(a, b, d, e)	Ukladá riadenie rizík zmien IKT
Nariadenie EÚ DORA	Články 5, 8, 12	Upravuje prevádzkové riziko/IKT riziko a nahlasovanie incidentov
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Štruktúrované riadenie IT zmien, súlad a súvisiace požiadavky

1. Účel

1.1. Táto politika ustanovuje formálny rámec na iniciovanie, posudzovanie, schvaľovanie, implementáciu a preskúmanie zmien informačných systémov, infraštruktúry, aplikácií a súvisiacich procesov organizácie.

1.2. Zabezpečuje, aby sa všetky zmeny vykonávali riadeným a auditovateľným spôsobom, čím sa minimalizuje riziko narušenia prevádzky, oslabenia bezpečnosti alebo nesúladu s regulačnými požiadavkami.

1.3. Podporuje kontrolu 8.32 prílohy A normy ISO/IEC 27001:2022 tým, že vyžaduje bezpečné a zdokumentované postupy riadenia zmien zohľadňujúce riziká.

1.4. Politika zároveň zabezpečuje sledovateľnosť rozhodnutí o zmenách a podporuje prevádzkovú odolnosť pri plánovaných aj núdzových úpravách.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky zmeny ovplyvňujúce systémy, údaje a prostredia v rozsahu ISMS vrátane:

2.1.1. IT infraštruktúry (on-premise, cloudovej, hybridnej)

2.1.2. produkčných, predprodukčných a havarijných prostredí

2.1.3. podnikových aplikácií, služieb, rozhraní API a integrácií

2.1.4. nastavení konfigurácie, záplatovania, vydaní softvéru a migrácií systémov

2.1.5. núdzových opráv a projektových alebo plánovaných zmien

2.2. Upravuje zmeny iniciované:

2.2.1. internými zamestnancami (IT prevádzka, vývojári, vlastníci systémov)

2.2.2. externými dodávateľmi, poskytovateľmi riadených služieb (MSP) a zmluvnými pracovníkmi

2.2.3. projektovými tímami počas implementácie systémov, aktualizácií alebo prechodov služieb

2.3. Táto politika sa nevzťahuje na:

2.3.1. dočasné testovacie alebo vývojové prostredia bez prístupu k produkčným údajom

2.3.2. osobné používateľské konfigurácie (upravované v Politike prijateľného používania)

2.3.3. zmeny systémov mimo hraníc riadenia organizácie, pokiaľ neovplyvňujú integrované aktíva alebo povinnosti v oblasti súladu

3. Ciele

3.1. Zabezpečiť, aby boli všetky zmeny pred vykonaním preskúmané, schválené, otestované a zdokumentované.

3.2. Udržať dostupnosť systémov, integritu údajov a kontinuitu služieb počas činností súvisiacich so zmenami aj po ich vykonaní.

3.3. Vyžadovať pre všetky typy zmien definovanú klasifikáciu zmien, plány vrátenia zmien a posúdenia rizík.

3.4. Umožniť transparentné rozhodovanie a eskaláciu prostredníctvom štruktúrovaného riadenia.

3.5. Podporiť pripravenosť na audit prostredníctvom sledovateľných záznamov o zmenách a preskúmaní po implementácii.

3.6. Presadzovať oddelenie povinností a znižovať riziko neautorizovaných alebo konfliktných zmien v kritických systémoch.

4. Roly a zodpovednosti

4.1. Vrcholový manažment

4.1.1. Schvaľuje Politiku riadenia zmien a zabezpečuje jej súlad so strategickými cieľmi a regulačnými povinnosťami.

4.1.2. Schvaľuje programy zmien s vysokým dopadom alebo medzifunkčným dosahom v rámci správy a riadenia.

4.1.3. Prideľuje potrebné zdroje a rozpočet na nástroje riadenia zmien a školenia personálu.

4.2. Rada pre zmeny (CAB)

4.2.1. Preskúmava a schvaľuje štandardné a významné zmeny a zabezpečuje primerané vyhodnotenie rizík, dopadov a závislostí.

4.2.2. Potvrdzuje plány vrátenia zmien, výsledky testovania, komunikáciu so zainteresovanými stranami a harmonogram.

4.2.3. Tvoria ju vlastníci systémov, zástupcovia informačnej bezpečnosti, IT prevádzky, biznis lídri a zástupcovia súladu.

4.2.4. Za zdokumentovaných podmienok môže delegovať rozhodnutia o nízkorizikových alebo núdzových zmenách.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1. Spúšťače a frekvencia preskúmania

9.1.1. Táto politika musí byť preskúmaná raz ročne alebo pri:

9.1.1.1. významných zmenách IT alebo infraštruktúry

9.1.1.2. významných incidentoch súvisiacich so zlyhanými alebo neautorizovanými zmenami

9.1.1.3. regulačných aktualizáciách alebo nových právnych povinnostiach súvisiacich so zmenami

9.1.1.4. zavedení nových nástrojov alebo platforiem CMS

9.2. Proces preskúmania Politiky riadenia zmien

9.2.1. Manažér zmien vedie proces preskúmania v spolupráci s:

9.2.1.1. IT, informačnou bezpečnosťou a prevádzkou

9.2.1.2. interným auditom a riadením rizík

9.2.1.3. zástupcami CAB

9.2.2. Aktualizácie musí preskúmať a schváliť vrcholový manažment a Riadiaci výbor ISMS.

9.2.3. Opätovne vydané verzie musia byť evidované v registri dokumentov a oznámené dotknutým stranám; podľa potreby sa musí vykonať opätovné potvrdenie oboznámenia sa.

9.3. Riadenie dokumentov a verzií

9.3.1. Všetky verzie musia obsahovať:

9.3.1.1. identifikátor politiky, názov a klasifikačný stupeň

9.3.1.2. vlastníka a históriu revízií

9.3.1.3. záznam zmien a dátum účinnosti

9.3.1.4. schvaľovaciu autoritu

9.3.2. Archivované verzie sa musia uchovávať v súlade s Politikou uchovávania dokumentov (minimálne 3 roky).

10. Súvisiace politiky a väzby

10.1. Táto politika je priamo prepojená s týmito politikami a podporuje ich uplatňovanie:

10.1.1. P1 – Politika informačnej bezpečnosti: Ustanovuje požiadavku na formálne bezpečnostné kontroly a zodpovednosť na úrovni procesov vrátane správy a riadenia zmien.

10.1.2. P2 – Politika rolí a zodpovedností správy a riadenia: Definuje schvaľovacie právomoci a oddelenie povinností relevantné pre schvaľovanie zmien a dohľad.

10.1.3. P4 – Politika riadenia prístupu: Zabezpečuje, aby prístupové oprávnenia osôb vykonávajúcich a preskúmavajúcich zmeny zodpovedali zásade minimálnych oprávnení.

10.1.4. P6 – Politika riadenia rizík: Zabezpečuje, aby všetky zmeny podliehali primeranému vyhodnoteniu rizík a stratégiám zmiernenia.

10.1.5. P33 – Politika monitorovania auditu a súladu: Upravuje validáciu a auditné preskúmanie záznamov a porušení v oblasti riadenia zmien.

10.2. Tieto politiky spoločne umožňujú obhájiteľný, sledovateľný a bezpečný životný cyklus riadenia zmien v rámci ISMS.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001:2022

11.1.1. Kapitola 6.1 – Opatrenia na riešenie rizík a príležitostí: Táto politika podporuje identifikáciu, vyhodnotenie a riadenie rizík súvisiacich so zmenami.

11.1.2. Kapitola 5.15 – Riadenie prístupu: Zabezpečuje, aby bol prístup počas zmien riadený a sledovateľný.

11.1.3. Kontrola 8.32 prílohy A – Riadenie zmien: Táto politika v plnom rozsahu implementuje požiadavku riadiť zmeny zariadení na spracovanie informácií a systémov plánovaným a riadeným spôsobom.

11.2. ISO/IEC 27002:2022 – Kontrola 8

11.2.1. Posilňuje implementáciu štruktúrovaného procesu riadenia zmien vrátane klasifikácie zmien, schvaľovania, testovania, vrátenia zmien a dokumentácie.

11.3. NIST SP 800-53 Rev.5

11.3.1. Rodina CM (CM-1 až CM-14): Táto politika je úzko zosúladená s kontrolami riadenia konfigurácie vrátane referenčných konfigurácií (CM-2), riadenia konfiguračných zmien (CM-3), analýzy bezpečnostných dopadov (CM-4) a obmedzení prístupu (CM-5).

11.3.2. Rodina AU (AU-2, AU-6, AU-12): Mechanizmy logovania a auditu uvedené v tejto politike podporujú sledovateľnosť udalostí a preskúmanie súladu pre činnosti súvisiace so zmenami.

11.3.3. RA-3, RA-5: Posúdenia rizík vyvolané zmenami a skeny zraniteľností sú začlenené do procesu vyhodnocovania zmien.

11.3.4. PM-11 (Definícia poslania/podnikových procesov): Zabezpečuje, aby boli počas zmien zachované ciele kontinuity podnikania a prevádzkové ciele.

11.4. Nariadenie EÚ GDPR (2016/679)

11.4.1. Článok 32(1)(b–d): Táto politika podporuje požiadavku na primerané technické a organizačné opatrenia na zabezpečenie bezpečnosti údajov, najmä počas zmien systémov.

11.4.2. Článok 25 – Ochrana údajov už v štádiu návrhu a štandardne: Zabezpečuje, aby zmeny ovplyvňujúce osobné údaje integrovali ochranu súkromia a bezpečnosť do návrhu a nasadenia.

11.4.3. Odôvodnenie 78: Vyžaduje, aby prevádzkovatelia zaviedli mechanizmy, ako sú politiky riadenia zmien, na zabezpečenie priebežnej dôvernosti, integrity a odolnosti systémov spracúvania.

11.5. Smernica EÚ NIS2 (2022/2555)

11.5.1. Článok 21(2)(a, b, d, e): Ukladá technické a organizačné opatrenia na riadenie rizík IKT vrátane rizík vyplývajúcich zo zmien systémov, aktualizácií softvéru a úprav infraštruktúry.

11.6. Nariadenie EÚ DORA (2022/2554)

11.6.1. Článok 5 – Rámec správy a riadenia a vnútorných kontrol: Táto politika presadzuje zásady riadenia prevádzkových rizík naviazané na zmeny a aktualizácie IKT.

11.6.2. Článok 8 – Rámec riadenia rizík IKT: Ukladá, aby finančné subjekty riadili všetky zmeny ovplyvňujúce systémy IKT v rámci štruktúrovaných procesov riadenia zmien, čo sa v tejto politike odráža v požiadavkách na klasifikáciu, testovanie, vrátenie zmien a dokumentáciu.

11.6.3. Článok 12 – Nahlasovanie incidentov: Zabezpečuje, aby zlyhané zmeny vedúce k narušeniam IKT boli sledovateľné, zdokumentované a tam, kde je to relevantné, nahlásené.

11.7. COBIT 2019

11.7.1. BAI06 – Riadené IT zmeny: Táto politika priamo napĺňa ciele BAI06 ustanovením štruktúrovaných workflow na schvaľovanie zmien, posudzovanie dopadov, komunikáciu a testovanie.

11.7.2. BAI02 – Riadená definícia požiadaviek a BAI03 – Riadená identifikácia a tvorba riešení: Zabezpečujú, aby boli zmeny vychádzajúce z potrieb podnikania preskúmané a implementované bezpečne.

11.7.3. DSS01 – Riadená prevádzka: Podporuje priebežnú integritu systémov počas vykonávania zmien.

11.7.4. MEA01 a MEA03 – Monitorovanie, hodnotenie a posudzovanie výkonnosti a súladu: Umožňuje nepretržitý dohľad nad účinnosťou Politiky riadenia zmien a jej uplatňovaním.